(6)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 63-220684
(43)Date of publication of application : 13.09.1988

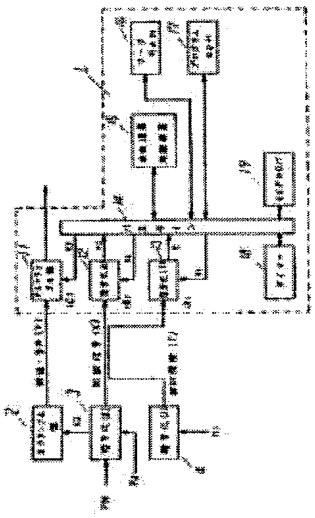
(51)Int.Cl. H04N 7/16
H04H 1/00

(21)Application number : 62-054558
(22)Date of filing : 10.03.1987

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : HIRASHIMA MASAYOSHI

(54) TERMINAL CONTROL SYSTEM

(57)Abstract:
PURPOSE: To continuously receive only formal terminal of which procedure is finished by previously sending a next key which becomes effective in a fixed term to a tariff prepayment terminal, canceling a former key with the aid of timer output and writing a new key in a decoder.
CONSTITUTION: When a timer 18 automatically generates an off-signal at the end of a month or the beginning of a month and stops sending an cipher key K2 to the decoding part 12, the decoding part 12 can not decode. Therefore a cipher key K3 cannot be obtained and both of an image and a voice cannot be decoded. On the other hand, the ciphered information on a next month pay ment, the key K2 and time information are simultaneously sent with a terminal address to the terminal in which the next month tariff is paid for until a fixed date from a center. Thus after passing the fixed term, the tariff non-payment terminal automatically cannot decode the cipher.



(6)

訂正有り

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　昭63－220684

⑤Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和63年(1988)9月13日
H 04 N 7/16		C－8321－5C	
H 04 H 1/00		F－7608－5K	

審査請求　未請求　発明の数 1　(全7頁)

⑭発明の名称　端末制御方式

⑳特　願　昭62－54558
㉒出　願　昭62(1987)3月10日

㉑発明者　平嶋　正芳　大阪府門真市大字門真1006番地　松下電器産業株式会社内
㉑出願人　松下電器産業株式会社　大阪府門真市大字門真1006番地
㉔代理人　弁理士　中尾　敏男　外1名

明　細　書

1、発明の名称

端末制御方式

2、特許請求の範囲

(1) 多数の端末器をセンターから制御できる情報伝送システムにおいて、端末器内に、第1の暗号化鍵K_1で暗号化された時刻情報を復号化する機能Aと、第2の暗号化鍵K_2で暗号化された端末制御信号Xを復号化する機能Bと、第3の暗号化鍵K_3で暗号化された情報Yを復号化する機能Cとを有し、機能Bにより、機能Cの動作を停止或は開始させる事を特徴とする端末制御方式。

(2) 機能Bの復号出力K_3をEEPROMにメモリーし、機能A，B，Cを実行させるプログラムを書込んだROMと機能A，B，Cを実行するハードウェアの一部又は全部とこれらを制御する中央演算処理部と上記EEPROMと、上記EEPROMとを同一基盤上に集積化し、密封し、開封しても顕微鏡等により拡大しない限り上記A，B，Cを実行するハードウェア，EEPROM及びROMのレイアウト，回路構成が判別できないような集積回路素子を用いてなる特許請求の範囲第1項記載の端末制御方式。

(3) 第1の鍵K_1と第2の鍵K_2を共通にした事を特徴とする特許請求の範囲第1項又は第2項記載の端末制御方式。

3、発明の詳細な説明

産業上の利用分野

本発明はCATV或は衛星放送等で有料放送を実施する場合の料金不払端末の制御と、料金支払済端末を聴視可に設定することができる端末制御方式に関するものである。

従来の技術

CATV或は衛星放送等に利用されるシステムにおいては、料金未払端末に、強制オフ信号を送って、聴視不可としていた。また、盗聴を防止するために多層鍵による方式も考えられている。

発明が解決しようとする問題点

しかしながら、上記のような多層鍵による方式

3 ページ

は構成が複雑になる等、以下のような不都合を有していた。

(1) 強制オフ信号を各端末毎に送る場合、端末が電源オフされていれば、オフにできないので、オフ情報を絶えず送り続けねばならず、端末が多くなると、その端末がアクセスされて、オフされるまでに相当の時間が必要となり、その間不正聴視が可能である。例えば、１フィールドで一端末をアクセスすると、１日２４時間で５１８万４千端末をアクセスできる。仮に全国３千万世帯中１%が毎月不払いとなれば３０万世帯をアクセスする必要があり、１時間で２１万６千世帯だから約１時間半毎に１回アクセスできる。従って不払いでも平均して約$\frac{1}{2}$×９０分、即ち４５分は不正に見られるので、５分或は１０分見る毎にオフレオフ期間を長くすれば、料金未払いでも視聴できる。

(2) 毎月、月末，月始めに、端末をオンする情報を送る場合、各端末のアドレスをアクセスする為には、加入者３千万で１フィールド毎に一端末をアクセスすると約６日必要となり、端末が約１週間連続通電される必要がある。端末のＡＣコードがこの間に抜かれているとオン情報は伝わらない。

(3) タイマーを内蔵し、月末に自動オフする方式ではタイマーの電源がオフになると誤動作する。

本発明は上記問題点に鑑み、不正聴取が困難な端末制御方式を提供せんとするものである。

問題点を解決するための手段

本発明は上記目的を達するため、多数の端末器をセンターから制御できる情報伝送システムにおいて、端末器内に、第１の暗号化鍵K_1で暗号化された時刻情報を復号化する機能Ａと、第２の暗号化鍵K_2で暗号化された端末制御信号Ｘを復号化する機能Ｂと、第３の暗号化鍵K_3で暗号化された情報Ｙを復号化する機能Ｃとを有し、機能Ｂにより、機能Ｃの動作を停止或は開始させる構成となっている。

作用

本発明は上記した構成により、料金未払端末鍵

5 ページ

K_2による復号を停止すると共に、料金前納端末に、次の一定期間有効となる鍵を予め送っておき、タイマー出力で前の鍵をキャンセルし、新しい鍵を復号器へ書込むことで、正規の手続済端末のみ継続して受信でき、料金支払済期間終了後は、未払端末は受信不能となる。

実施例

本発明の一実施例を第１図に示す。第２図のϕ_1，ϕ_2に伝送信号のフォーマットを示す。１パケット中ヘッダー１６ビット，メッセージ１９０ビット，訂正ビット８２ビットとすると文字放送のＢＥＳＴ方式が使える。本発明の動作の概要を述べる。端末をアクセスする場合、先ず時刻コードＴをＤＥＳで暗号化し、第２図に示すϕ_1のメッセージの中へ６４ビットで入れて送る。暗号化及復号化は共通鍵K_1で行えるものとし、各端末とセンター間は一対で、端末の数だけ鍵があるものとする。時刻コードを復号化部１３で復号化し、タイマー１８を校正する。校正は端末アクセスの都度行うものとする。又、同時に１９０－６４＝

6 ページ

１２６ビットの他のメッセージも送られる。ここで端末アドレスを暗号化せずに入れておいてもよい。タイマー１８からオフ情報が出る迄、鍵K_2で暗号化されたＰＮコード、即ち制御信号Ｘは復号化部１２で復号化される。復号化部１２の出力のK_3で、スクランブルされた映像及音声信号を復号（デスクランブル）し、映像，音声を得る。

以下、第１図～第３図と共に更に詳しく述べる。第２図のϕ_1，ϕ_2又はϕ_3はＶＢＬ中の１０～１７Ｈに８パケット分重畳されるものとし、各端末への時刻情報はK_1で暗号化されているので不正視聴のため、処理回路１へ、偽の時刻情報を入力する事はＤＥＳを解く事になり実質的に不可能である。

第３図において２５は同期再生回路、２２は第１０～１７Ｍの各Ｈの水平走査期間に重畳されたϕ_1の各２８８ビットのみを抜取る抜取回路、２３は抜取回路２２の出力をパルスに整形する２値整形回路、２４はＩＣ化されたＢＥＳＴ方式の誤り訂正回路で、１フィールド内に８パケット処

理できるものである。（１フィールド１パケットの処理能力なら、誤り訂正回路２４はＬＳＩにすればよい。）誤り訂正回路２４の出力が暗号解読処理回路１′の復号化部１２，１３へ供給される。暗号解読処理回路１′は第１図の処理回路１から、ビデオメモリ１１Ｍ，復号制御回路１１Ｖ，音声再生回路１１Ｓを除いた部分である。尚、復号制御回路１１Ｖはビデオメモリ１１Ｍからの読出しを制御するもので、音声再生回路１１ＳはＰＣＭ復調と、ＰＣＭ復調出力の暗号解読を行なう回路である。

さて、映像信号を第３図に示すＤＥＴ２１で検波して取り出す。仮に衛星放送とすれば、ＤＥＴ２１はＦＭ検波回路である。ＤＥＴ２１の出力中の例えば、5.73Ｍの音声キャリアを音声再生回路１１Ｓで復調する。音声がＰＣＭの時、ディジタル処理は容易であり、第１図のスクランブル部２で、暗号化されたＰＮ信号K_3で暗号化して送られる。映像は、ランダム反転或はラインバーミュティション等K_3を用いて暗号化される。映像信号はビデオメモリ１１Ｍに記憶される。ビデオメモリ１１Ｍは１フィールド分でも、それ以下の容量のものでも又、アナログでもディジタルでも差仕えない。一方、K_3を得るためのK_2は、例えば１カ月（２カ月或は0.5カ月毎）に変化するものとすれば、タイマー１８からオフ情報が出ない限り、ＣＰＵ１５とワークＲＡＭ１６，プログラムＲＯＭ１７の内容による処理によって、K_2が復号化部１２へ伝えられており、第３図に示す復号化部１２，１３へ誤り訂正された各パケットのメッセージが入力され、復号され、ＣＰＵ１５，ワークＲＡＭ１６，プログラムＲＯＭ１７で判定され、必要な情報K_3等がワークＲＡＭ１６の一部へメモリされる。さて、タイマー１８で、月末又は月始め（毎月１日零時零分）にオフ信号を自動的に発生させ、即ちＣＰＵ１５，ワークＲＡＭ１６，プログラムＲＯＭ１７でこれを判定，検出し、バスライン１４を介して、復号化部１２へ鍵K_2を送るのをやめると、復号化部１２では復号できなくなり、K_3が得られず画像，音声共に復

号できなくなる。一方、所定期日迄に翌月の料金を支払った端末には、センターから端末アドレス（非暗号化）と共に、第２図のϕ_1の如く暗号化して、翌月分支払済情報と鍵K_2を時刻情報と共に送る。即ち、アドレス３０ビットで１０億個まで端末判別でき、暗号化された８８ビットの料金情報で、何月分か、何円払ったか、どんなジャンル，番組を見たいか等々の情報と鍵K_2が送られる。これらの情報を月末までに受信し、EEPROM１９の所定の位置にメモリしている時はタイマー１８より、オフ信号が出力されても、ＣＰＵ１５，ワークＲＡＭ１６，プログラムＲＯＭ１７は、その信号を無視し、次の月のK_2を復号化部１２へ与える。このような動作は、全部プログラム処理しても、全部ハードロジックで処理しても、両者混合してもよい。料金情報をＥＥＰＲＯＭ１９へ書込むので、受信機のＡＣ電源がオフになっても、タイマー１８がバッテリーバックアップで、そのバッテリーが除去されたとしても、ＥＥＰＲＯＭ１９の内容は保持されるので、再び電源を供給す

れば、ＥＥＰＲＯＭ１９からK_2を読み出すことができる。

上記の説明では、時刻コードが不正解読されないよう各端末毎に、その端末をアクセスする都度、タイマーを較正したが、時刻コードは全端末共通の鍵K_1（以下前の説明と区別するためK_1'と記す）で暗号化する場合を考える。K_1'は送受システム運用者及び機器製造者が知り得るがK_1'を知って時刻情報を偽造し、第３図の誤り訂正回路２４の出力の代りに、暗号解読処理回路１′へ入力しても、料金情報及鍵K_2を別の鍵K_0で暗号化し、K_0を端末毎に別々にすれば、第２図のϕ_1，ϕ_2の形と同一の秘密性が保たれる。この場合、端末アクセス中はϕ_5を７Ｈ、ϕ_5は１Ｈに重畳し、毎分１回ϕ_4をϕ_5の代りに送る。端末非アクセス時は、８Ｈ共ϕ_5を重畳し、毎分１回ϕ_4をϕ_5の代りに送る。この時、受信側は、第４図の如くなる。第４図は主要部を示し、誤り訂正回路２４でϕ_1～ϕ_5のメッセージ１９０ビットを誤り訂正し、バッファメモリ３３へメッセージ

１９０ビットをメモリさせる。バッファメモリ３３の内容を中央演算処理装置１５と、ワークＲＡＭ１６，プログラムＲＯＭ１７により判定する。まず制御の８ビットでパケットの種類ϕ_3かϕ_4かϕ_5かを判定し、ϕ_4の時、最初の６４ビットをK_1'で復号する。この６４ビット中の時刻コード３９ビットをバスライン１４を介してタイマー１８へ書込む。この時、中央演算処理装置（以下ＣＰＵという）１５より、Ｉ／Ｏポート（出力ラッチ付）を低レベルとして、バスライン１４のデータ，アドレスをタイマー１８へ入力可とし、フリップフロップ（以下ＦＦという）３２をリセットする。電源オン時、主電源の立上りのエッヂで、ＦＦ３２がセットされているので、Ｑが低レベルになっており、これが、Ｉ／Ｏポート３０を介し、ＣＰＵ１５へ伝えられているので、タイマー１８へϕ_4の中の時刻コードを１回書込むと、ＦＦ３２のＱが高レベルになって、ＣＰＵ１５の入力ポートが高レベルになる。従って、以降ϕ_4は無視する。以降タイマー１８から例えば

尚、このアクセス時間について簡単に説明すると、８パケットの場合、７パケットをアクセスに、１パケットは制御用に使うと、１パケット一端末として、

６０×６０×７＝２５２００／分

１５１.２万端末／時間

３６２８.８万／日

アドレスを２５ビットとし、３２００万端末に制限し時刻コードをＢＣＤで現わし、年は８ビット、月は４ビット＋１ビット、日は４ビット＋２ビット、時は４ビット＋２ビット、分は４ビット＋３ビット、秒は４ビット＋３ビットとすると全部で３９ビットとする。１アドレス当り料金情報を２７ビットにすると、１パケット１９０ビット中制御信号８ビットを除く１８２ビットが（２５＋３９＋２７）×２となり、２端末を１パケットでアクセスでき、１時間当り３０２.４万／時間即ち、３０００万なら１０時間でアクセスできる。アドレス以外の各６６ビットをＤＥＳで暗号化するのは、ϕ_1もϕ_0も同一の考え方である。

１時間毎に、信号（５９分００秒）をバスライン１４を介して取り出し、ＣＰＵ１５で、バッファ３３にϕ_4のデータがメモリされるのを待つ。タイマー１８の誤差は、タイマー１８を水晶で構成すれば月差１５秒程度となるので、電源オン時に１回、時刻を較正すれば、以降６０分毎に、時刻コードを取り込みタイマー１８を較正する。送信側で、予め毎時００分の前後１～２分間、重要情報を送らなければＤＥＳの鍵K_1'を用いて、時刻コードを復号する事にＣＰＵ１５，ワークＲＡＭ１６，プログラムＲＯＭ１７を専念させ得る。それ以外の期間で、ＤＥＳによる復号を行なうのは端末がアクセスされた時、つまり月１回のみである。従って、送り側でＤＥＳにより暗号化した信号を送る時、その後、一定時間、端末にとって重要な信号を送らないか、何回も続けて送るかして受信側でＤＥＳ復号中に重要信号を検出洩れすることは無い。また、ϕ_5の如く１パケット内に３端末分のデータを送ることもでき、アクセス時間は短かくできる。

尚、タイマー時刻については、電源オン時に必ず１回較正し、以降一定の間隔でタイマーを較正するようにしても良い。

発明の効果

以上の如く、本発明により、一定期間経過後、料金不払端末は自動的に暗号化の解読ができなくなり、不正解読は極めて困難で、以下に示す効果も得られるものである。

(1) タイマーで、料金不払端末の動作を停止。

(2) タイマーの構成信号は暗号化してあり解読できない。

(3) 比較的長期間使用の鍵をＥＥＰＲＯＭに入れるので、電源がオフになっても、鍵が残る。

(4) ＤＥＳによる時刻情報の復号化を１時間に１回としておいても電源オン時１分以内に、タイマーが較正され、かつ、ＤＥＳ復号時間を短かくできる。

４、図面の簡単な説明

第１図は本発明の一実施例における端末制御方式を具現化する端末制御装置のブロック図、第２

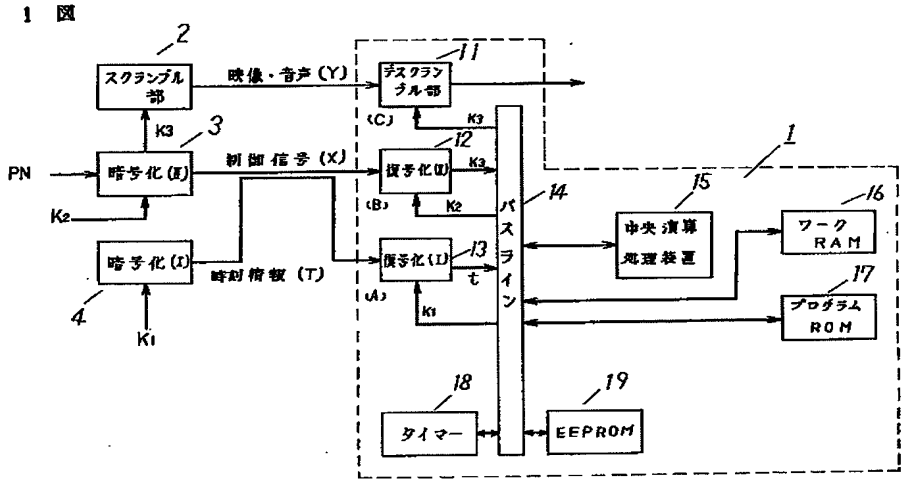
１５ ページ

図は同パケット構成を示す状態図、第３図，第４図は同装置の概略構成を示すブロック図である。

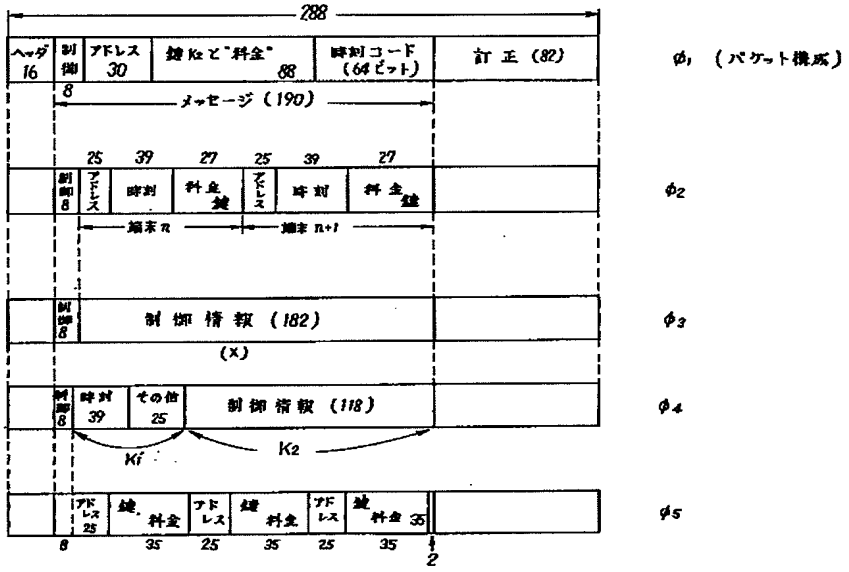
１……信号処理部、２……スクランブル部、３，４……暗号化部、１１……デスクランブル部、１２，１３……復号化部、１４……バスライン、１５……中央演算処理装置、１６……ワークＲＡＭ、１７……プログラムＲＯＭ、１８……タイマー、１９……ＥＥＰＲＯＭ。

代理人の氏名　弁理士　中　尾　敏　男　ほか１名

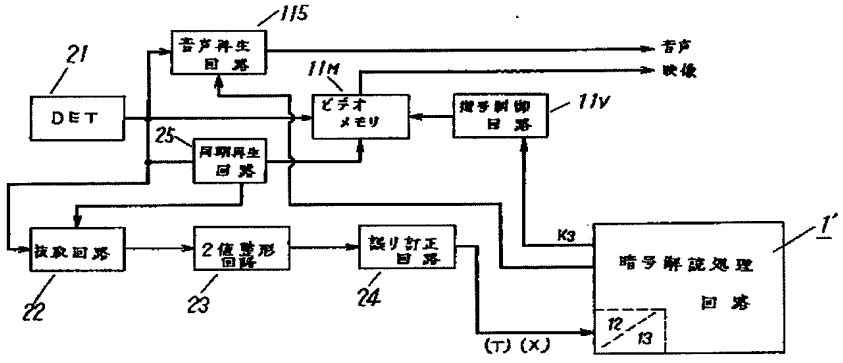
第　１　図



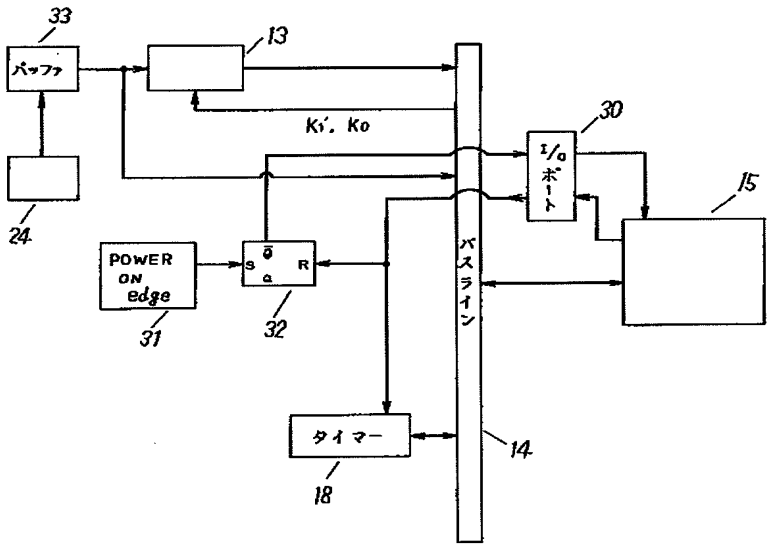
第 2 図


288
ヘッダ 16
制御
アドレス 30
鍵 K2 と"料金" 88
時刻コード (64ビット)
訂正 (82)
φ1 (パケット構成)
8
メッセージ (190)
25 39 27 25 39 27
制御 8
アドレス
時刻
料金 鍵
端末 n
端末 n+1
φ2
制御情報 (182)
(X)
φ3
時刻 39
その他 25
制御情報 (118)
K1
K2
φ4
アドレス 25
鍵
料金 35
φ5
2

第 3 図


115
音声再生回路
音声
映像
21
DET
11M
ビデオメモリ
信号制御回路
11V
25
同期再生回路
抜取回路
2値整形回路
誤り訂正回路
K3
暗号解読処理回路
1'
12
13
(T) (X)
22
23
24

第 4 図


33
バッファ
13
K1'. Ko
30
I/O ポート
15
24
POWER ON edge
S Q R
31
32
バスライン
タイマー
14
18